NASA Procedural Requirements

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

Chapter 11 Security Controls

11.1 Controls

11.1.1 Security controls are selected based on the outcome of the analysis of the IT system's security objectives. The selection of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization. Security controls are the management, operational, and technical safeguards and countermeasures prescribed for an information system which, when taken together, adequately protect the confidentiality, integrity, and availability of the system and its information.

11.1.2 Given the magnitude of risks inherent in IT operations and the cost associated with IT security controls, all risks can rarely be eliminated. Therefore, a risk management-based approach must be used that finds the right balance between operational needs, limited budgets, identified risks, and available security controls.

11.2 NIST Security Controls

11.2.1 NIST SP 800-53, Recommended Controls for Federal Information Systems, provides a complete catalog of baseline controls based on the impact levels of low, moderate, and high to ensure the confidentiality, integrity, and availability of the system. Based upon the selected IT security category (see Section 7.2, Categorization of Information), specific security controls from NIST SP 800-53 are required to be evaluated against the specific mission and line of business objectives. If the security controls are appropriate for the system, they must be designed into the architecture of the system and system IT security strategy.

11.2.1.1 The baseline set of security controls is the initial starting point. Information system owners must be prepared to increase this set of baseline controls to protect their systems as warranted by their additional requirements or as required by NASA-wide security controls. (See Section 11.3, NASA-wide Common Security Controls.)

11.2.1.2 During the controls selection process, information system owners must continually review their information and information system security strategy. (See Chapter 6, Information and Information System IT Security Strategy.)

11.2.2 NIST Security Controls Requirements

11.2.2.1 All master and subordinate systems shall document, in the Review of Security Controls section of their SSP, the NIST SP 800-53 security controls recommended for the system's IT security category and provide the following information in a Security Controls Assessment Table:

a. NIST control number.

b. Applicability determination (Yes, No, Not Applicable).

c. Control Name.

d. Control Implementation Description.

e. Implemented (Yes/No and Date).

f. Assessment Method used to determine that the control was implemented.

g. Initials of individual that determined it was or was not implemented.

h. Comments.

11.2.2.2 The Security Controls Assessment Table shall follow the example format in Figure 11-1. The table can be either in the body of the SSP or included as an appendix to the SSP. The table should present the Control Numbers in the same order as presented in NIST SP 800-53, Recommended Controls for Federal Information Systems, Appendix F.

Control No.	Y, N, N/A	Control Name	Control Implementation Description	Implemented and Tested (Y/N) and Date	Assessment Method	Initials	Comments
AC-1	*N*	*ACCESS CONTROL POLICY AND PROCEDURES*		*No.*	*Verify documentation.*	*JRR*	*Risk accepted for pilot Proof-of-concept system, which will only be operational 2 months.*
AC-2	*Y*	*ACCOUNT MANAGEMENT*	*System SOP used to establish the process for account management. All accounts have to be revalidated annually by NASA sponsor and users required to re-sign appropriate use statement.*	*Yes. May 2005*	*Reviewed SOP and check account forms for signatures not over 1 year old.*	*JRR*	*Accounts are not annually reviewed because the length of Proof-of-concept operation is 2 months.*

Figure 11-1 Sample Security Controls Assessment Table

11.2.2.3 All security controls determined to be non-applicable to the system shall have the reason for the non-applicability documented in the comments section of the Security Controls Assessment Table and concurred or non-concurred on by the Center ITSM.

11.2.2.4 All security controls that are not implemented, but are applicable to protect the information or the information system, shall be documented as residual risks and tracked in the POA&M for the system.

11.2.2.5 Each control that has not been implemented and has been risk accepted by the AO shall be identified in the comments section of the Security Controls Assessment Table.

11.2.3 NASA-Defined Parameters for NIST Security Controls

11.2.3.1 Some of the security controls in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, Appendix F, Security Control Catalog, provide a degree of flexibility by allowing organizations to define input values for certain parameters associated with the control. This flexibility is achieved using assignment and selection operations within the main body of the control statement. Once specified, the organization-defined value becomes part of the security control, and the organization is assessed against the completed control statement.

11.2.3.2 Responsibility for determining the assignment and selection organizational operational parameters is at the master system level if the controls have not been established as NASA-wide common security controls.

11.2.4 NASA-Defined Parameters for NIST Security Controls Requirements

11.2.4.1 NASA shall define in each master system the optional parameters (i.e., assignment and selection) that will be used by the master system and inherited by its subordinate systems. These parameters will be:

a. Documented in the subordinate system's Security Controls Assessment Table.

b. Verified or tested for implementation during self-assessments of the system.

11.2.4.2 Subordinate systems, for which a master system has not been established, shall assign the security

controls parameters, document the selections in the Security Controls Assessment Table of the SSP, and verify or test the security control's implementation during self-assessments of the system.

11.3 NASA-Wide Common Security Controls

11.3.1 NASA has the option to select and enforce certain security controls that shall be adopted by all NASA master and subordinate systems. The NASA SAISO shall publish at least annually a list of those controls that have Agency-wide applicability.

11.3.2 Background Screening of Personnel

11.3.2.1 All personnel granted physical or logical access, including remote logical access, to IT resources not intended for open access by the general public shall undergo background screening and adjudication in accordance with NPR 1600.1, NASA Security Program Procedural Requirements, prior to being granted access and periodically thereafter.

11.3.2.2 Exceptions to the requirements for personnel screening shall be granted by the OSPP in coordination with the OCIO.

11.3.3 Appropriate Use of IT Resources

11.3.3.1 A NASA appropriate use policy statement, based on NPD 2540.1, Personal Use of Government Office Equipment Including IT, and approved by the NASA General Counsel, shall be required from every individual granted access to NASA information systems and networks.

11.3.3.2 The use policy statement in Figure 11-2 shall be the NASA standard.

> Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

Figure 11-2 Appropriate Use Policy Statement

11.3.3.3 Exceptions and modifications to the NASA appropriate use statement to comply with local laws shall be approved by the cognizant NASA General Counsel.

11.3.3.4 The applicable NASA appropriate use policy statement shall be agreed to and acknowledged by either signing the statement or by obtaining an electronic document from the individual acknowledging acceptance of the use policy.

11.3.4 Limited Personal Use of IT Resources

NPD 2540.1, Personal Use of Government Office Equipment, permits NASA employees limited use of IT resources for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. (See NPD 2540.1 for specific uses and restriction.)

11.3.5 Personally-Owned and Company IT Resources

11.3.5.1 Personally-owned IT resources and company-owned resources, utilizing a network IP address, are subject to all network security activities, such as content monitoring, penetration testing, and vulnerability scanning.

11.3.5.2 Personally-owned IT resources and company-owned resources, utilizing a NASA-managed network IP address, shall be approved by the Center NCCB.

11.3.5.3 Personally-owned and company-owned IT resources, utilizing a network IP address, shall comply with NPD 2540.1, Personal Use of Government Office Equipment.

11.3.6 Warning Banners

11.3.6.1 Government computer systems may be targets of hostile activities and subject to other forms of unauthorized use. To counter these activities, the Government may monitor and record the use of Government computer systems through keystroke monitoring and other methods. To deter misuse and notify all users that their use may be monitored, guidance is provided on implementing a warning banner on all appropriate NASA computer systems. This requirement applies to all NASA-owned or NASA-funded IT systems, regardless of location or user, including Government-provided equipment.

11.3.6.2 The NASA General Counsel-approved warning banner shall warn users that their computer, application, and network activities are subject to monitoring, their keystrokes may be monitored and logged, and there is no expectation of privacy. (See Figure 11-3)

> This US Government computer is for authorized users only. By accessing this system you are consenting to complete monitoring with no expectation of privacy. Unauthorized access or use may subject you to disciplinary action and criminal prosecution.

Figure 11-3 NASA-Approved Warning Banner

11.3.6.3 All computers and applications that are owned by or operated on behalf of NASA and requiring user authentication for access shall display and require acknowledgement of the NASA General Counsel-approved warning banner prior to logging on to a NASA system.

11.3.6.4 IT resources not owned by NASA nor operated on behalf of NASA, but utilizing an IP address assigned to NASA, shall be subject to the conditions contained in the NASA warning banner unless a waiver has been granted by the cognizant CIO.

11.3.6.5 Augmentations to the NASA warning banner, to comply with local laws, shall be approved by the NASA or Center Office of the General Counsel.

11.3.6.6 For the current version of the warning banner, see your Center ITSM.

11.3.7 Password Requirements

11.3.7.1 Passwords shall not be electronically transmitted without using encryption.

11.3.7.2 Passwords shall be changed at least annually.

11.3.7.3 Systems shall automatically enforce password attributes, if supported by the system or application.

11.3.7.4 Passwords attributes shall consist of:

a. Between 8 and 128 characters.

b. At least one special character, if supported by the system or application.

c. At least one character from each of the other three character sets: lower-case letters, upper-case letters, and numerals, if supported by the system or application.

11.3.7.5 All vendor-supplied passwords must be identified and changed prior to deployment.

11.3.7.6 Simple Network Management Protocol (SNMP) Community strings and other password-like mechanisms will follow the password requirements.

11.3.7.7 Passwords shall be reset whenever a user forgets a password, when evidence exists that a password may have been compromised, or when management believes that a reset is in the best interest of the security of the system.

11.3.7.8 Passwords attributes shall not consist of:

a. Repeating or consecutive sequence of characters.

b. Information about the user (i.e., username, user ID, office, or function).

c. Dictionary words (i.e., English or other language) even with numerals used to replace letters.

11.3.7.9 Exceptions to the password requirements shall be identified as residual risks and documented in the Accreditation Package presented to the AO.

11.3.8 Computer Support and Operations

11.3.8.1 Computer support and operations include both system administration and tasks external to the system that support its operation, such as maintaining documentation. It does not include system planning or design. The support and operation of any IT system are critical to maintaining the security of a system. Support and operations will include activities that enable IT systems to function correctly. These include fixing software or hardware problems, loading and maintaining software, and helping users resolve problems.

11.3.8.2 The failure to consider security as part of the support and operations of IT systems undermines security measures due to poor documentation, old user accounts, conflicting software, and poor control of maintenance accounts.

11.3.8.3 NASA computer support and operations shall:

a. Ensure that IT support and operations controls are continuously addressed, including hardware maintenance, software maintenance, system and information integrity, and media protection.

b. Implement controls to facilitate system maintenance and to ensure compliance with vulnerability reduction and patch management.

c. Ensure the development and implementation of processes for system access including:

(1) Determining the level of access and privileges a user is given to the information system.

(2) Determining specific processes for access by foreign nationals.

(3) Ensuring that system users and support personnel receive the required security training (e.g., instruction in rules of behavior).

d. Employ antiviral and protection mechanisms to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, removable media, downloaded code, or other methods.

e. Ensure that the computer infrastructure has built-in recovery features (availability), provides adequate baseline protections (confidentiality), and protects data from unauthorized modifications (integrity).

f. Ensure that all NASA systems and data are backed up on a schedule and methodology in accordance with system requirements based on the impact level of the loss of the data.

g. Ensure that mechanisms, in addition to auditing and analysis of audit trails, are implemented to detect unauthorized and illegal acts.

h. Ensure that all ACI or SBU information is categorized in accordance with FIPS 199 and protected in accordance with NIST SP 800-53.

i. Ensure that all required system documentation is:

(1) Maintained and up to date.

(2) Based on the type of system and its category, nature of the information, system software and hardware, applicable laws, FISMA requirements, and requirements for certification and accreditation.

(3) Marked and protected as ACI or SBU where appropriate. (See NPR 1600.1, NASA Security Program Procedural Requirements, for more information).

j. Ensure that all media are labeled with both a description and an appropriate sensitivity marking, such as non-sensitive, or Administratively Controlled Information (ACI), which includes Privacy Act, International Traffic in Arms (ITAR), Export Controlled, Company Proprietary, and information about the security or configuration of NASA IT resources and networks. (See NPR 1600.1).

k. Ensure that all excessed media is properly sanitized following the current NASA memorandum on the Sanitization of NASA Equipment prior to leaving NASA's custody. This can include the destruction of media in a facility rated for the type of information stored on the media.

l. Ensure that the Center/Mission Directorate network and IT security system support and operations staffs have the skills and resources necessary to identify security problems, respond appropriately, inform appropriate individuals, and assist users.

m. Ensure that there is a separation of duties for critical operations.

11.3.9 Internet Publishing Content Requirements

11.3.9.1 Publication via the Internet is defined as making information available to the public-at-large via the Transport Control Protocol/Internet Protocol (TCP/IP) network protocol without authentication. This includes, but is not limited to, hypertext transfer protocol HTTP (hypertext transfer protocol), associated protocols (i.e., World Wide Web), and anonymous File Transfer Protocol (FTP) traffic, as well as any other application (e.g., bulletin boards or

chart groups) that makes NASA information accessible to the public at large via IP.

11.3.9.2 NASA management and NASA personnel shall:

a. Comply with existing laws and policies that restrict the distribution of information.

b. Understand that all NASA information and data available to the public at large via the Internet, unless protected by appropriate access controls, are considered published and subject to the requirements of this document and references identified below.

11.3.9.3 All documents planned to be made available on the network shall be analyzed before publication against the guidelines listed in Figure 11-4 to ensure that they do not contain information that is inappropriate for public dissemination. Figure 11-4 is not all-inclusive, but is intended to provide examples of information that may be appropriate for publication.

Information Types	Examples
Documents Intended for General Dissemination	• The NASA Strategic Plan. • Strategic Plans and related documents. • Personnel locator information not covered by the Privacy Act or FOIA Exemption 6. This information includes, but is not limited to, Social Security numbers, home telephone numbers, home addresses, and medical data section. • Organizational information not covered by the Privacy Act or FOIA Exemption 6. • Directions to a Center and related information that meets the legitimate needs of the public wishing to visit our Centers. • Information intended by the Agency to assist the public in better understanding the Agency's history, organization, missions, programs, and projects. • Personal, work-related biographies may be made available on the network as long as they do not compromise any sensitive aspect of the project with which the individual may be associated.
Official Agency Web sites which provide Agency policy documents	• Agency policy documents via the NASA Online Directives Information System (NODIS).
Information released by the Agency and Center Public Affairs Offices	• Press releases and similar information. • Public service messages such as anti-drug campaign information.
Official Agency Information Approved for Release	• Information that must be made available electronically to the public per the provisions of the Electronic Freedom of Information Act. • Official Agency budget information to the level of detail approved for release by the CFO. • Information developed by the Agency to assist industry in doing business with NASA, including electronic commerce information that does not contain proprietary data or content sensitive information as per this document (e.g., Requests for Proposals (RFP) may be published, but offeror responses to RFPs or source selection information may not be published). • Vendor quotes as part of an electronic reverse auction.
Published Information	• Science and engineering information and data that compliy with NASA's policy for publication (see NPR 2200.2). • NASA Standards Program information, including official Agency engineering and information technology standards.

Figure 11-4 Information Appropriate for Publication on the Internet

11.3.9.4 The following information shall not be made available to the public at large via the Internet. If this information is made available via the Internet, security mechanisms shall be implemented to ensure that the information is available only to its intended, limited audience. Figure 11-5 is not all-inclusive but is intended to provide examples of information inappropriate for publication.

Information Types	Examples
Information critical to protecting NASA assets and personnel	• Computer passwords or pass phrases. • Computer network configurations or designs. • Identification of operating systems (vendor, product, and version) used on specific servers. • Internet Protocol addresses. • Telephone numbers for dial-up computer connections. • IT System capabilities (e.g., staffing levels, hours of operation) or limitations. • IT System security plans, risk analyses, system vulnerabilities, procedures, and controls methods. • IT System compromise information, including evidence data. • IT System security/auditing logs. • Names/telephone numbers that uniquely identify system administrators. • Physical security information such as key codes and cipher lock combinations and significant badging information, including pictures of NASA badges. • Internal Center maps, including labeled aerial views. • Technically-detailed schematics or drawings of utilities, networks, airfields, aircraft, and buildings. • Facility information, including detailed drawings, schematics, physical locations, staffing levels, and hours of operation. • Specific information on the composition, preparation, and storage locations or optimal use of hazardous materials, explosives, or bio-toxins. • Detailed disaster recovery plans. • Details on emergency response procedures, evacuation routes, or officials responsible for these issues. • Personnel locator information as contained in Center or Agency telephone books (e.g., mail stops or building numbers). • Internal Center policies and procedures that have unresolved content publishing issues. • Personnel locators (i.e., building and room numbers or other information which could be used to determine personnel whereabouts at a given point in time, e.g., calendar information). • Information on internal NASA-only or Center-only activities or events (e.g., picnics, symposiums), especially which specifies exact locations. • Non-work-related personal information (including links to personal web pages or resumes). • Date and time identification of security-sensitive events. • Video streaming or still images of locations where physical vulnerabilities might be exposed.

Information protected by law	• National security information (classified information).
	• Personal information prohibited from disclosure by the Privacy Act or FOIA Exemption 6. This information includes, but is not limited to, Social Security numbers, home telephone numbers, home addresses, and medical data.
	• Export-controlled information.
	• Technical innovations prior to release approval by patent counsel.
	• Proprietary information of the Government or others such as:
	  • Information disclosing inventions and technical innovations, including software, protected under 35 U.S.C. 205 and FOIA Exemption 3, unless release is approved by Center Patent Counsel.
	  • Trade secret information protected or prohibited from disclosure under the Trade Secrets Act (18 U.S.C 1905) or FOIA Exemption 4.
	  • Copyrighted materials unless approved for publication by the copyright owner.

	• Investigative information. • Commercially-licensed software restricted in accordance with the license or agreement under which it was obtained. • Information protected by treaty or agreement. • Invention disclosures. • Source evaluation information. • Confidential financial data relating to contractors. • Other information determined non-releasable under FOIA. • International Traffic in Arms Regulations (ITAR). • Procurement sensitive information, such as vendor quotes (except vendor quotes as part of an electronic auction), attribution information or results, or negotiating positions.
Information protected by Government or Agency policy or regulation	• NASA-developed software (unless authorized). • Information characterized as "Administratively Controlled Information" (per NASA policy) or previously designated "For Official Use Only." • Pre-decisional information such as the Agency budget prior to formal release.
Embargoed scientific, technical, launch or other mission information	• Launch-related information whose compromise may adversely impact safety or security.

Figure 11-5 Information Not Appropriate for Publication on the Internet

11.3.10 Use of Wireless Local Area Networks

11.3.10.1 The use of wireless local area networks (WLANS) provides wider capability to access the wired network through mobile computing devices. However, with the added benefits of wireless networking also comes additional risk. If implemented without the appropriate security controls, a wireless network can easily be exploited and used as a conduit for unauthorized network access, misuse, and abuse. Those responsible for the installation and operation of a wireless network must be aware of the inherent risks that exist in a wireless environment and its impact on a Center's Information Technology (IT) security posture.

11.3.10.2 Wireless Requirements

11.3.10.2.1 Wireless IT resources shall be designed and implemented to protect the confidentially, integrity, and availability of NASA's information.

11.3.10.2.2 All WLANs and wireless access points shall be approved by the Center NCCB and treated as part of the network infrastructure following all existing security and network standards, policies, and procedures. Adhoc networks are prohibited.

11.3.10.2.3 WLANs shall be monitored by the Center CIO.

11.3.10.2.4 All WLANs and wireless access points, architecture designs, and implementation shall follow NASA ITS-SOP-0020, Wireless Local Area Network Security Procedures.

11.3.10.2.5 Waivers for special circumstances shall be submitted for consideration to the Center NCCB and approved or disapproved by the Center CIO on a case-by-case basis. A security assessment and impact report shall be required for all waivers and documented in the appropriate SSP.

11.3.10.2.6 A full Center site survey shall be performed at least semi-annually to detect unauthorized WLAN access points. Spot checks for unauthorized WLAN access points shall be performed quarterly.

11.3.11 Peer-to-Peer (P2P) Connections

11.3.11.1 NASA shall follow OMB, Memorandum for CIOs' ; dated September 8, 2004; subject: Personal Use Policy and "File Sharing" Technology, which provides direction for establishing NASA P2P requirements.

11.3.11.2 Unapproved P2P file sharing technology has inherent security risks of downloading information from sites which may contain programs that pose considerable risks to NASA's IT infrastructure by introducing viruses, worms, Trojan horses, and other malicious code. Installing P2P software can make the system more vulnerable to compromises and unintended sharing of information from its hard drive. Federal law is clear and explicitly forbids the illegal distribution or other inappropriate use of copyrighted material.

11.3.12 P2P Requirements

11.3.12.1 Centers should actively prevent the use of unauthorized P2P file sharing.

11.3.12.2 The Center NCCBs shall implement port blocking and/or bandwidth/rate limiting to block or limit the most frequently used Internet ports for P2P file sharing applications. (Contact the Center ITSM for the most recent list of P2P ports.)

11.3.12.3 P2P file sharing technology shall only be utilized when approved, case-by-case, by the Center CIO or CIO designee and documented with the appropriate NCCB.

11.3.12.4 Unauthorized P2P traffic, once identified and traced back to a user by the Center ITSM, shall be blocked and the appropriate management notified to take appropriate administrative actions for the policy violation.

11.3.3 Network Security

11.3.13.1 Networks allow systems to connect for the sharing of data and files, as well as providing access to the resources themselves. The security architecture and configuration control of a network permits network connected systems to interact securely without jeopardizing their own security controls. Typically within NASA, there are WANs, LANs, WLANs, project-level networks, and network address translation (NAT) networks with private address space.

11.3.13.2 Each network is established to provide a different level of protection and typically connected in a layered fashion from the WAN to LAN to project level or NAT networks. Most NASA systems have a connection to a public network such as the Internet which is considered non-secure and presents threats that must be countered by security controls, vigilance, and monitoring. NASA systems that connect to networks operated by others shall review and concur on the protective measures and risk inherent in connecting to the network.

11.3.13.3 Network Security Requirements

11.3.13.4 All network architectures shall follow the NASA Enterprise Architecture which includes: border routers, firewalls, virtual private networks (VPNs), intrusion detection systems (IDS), and other associated network infrastructure. Guidance can be found in:

a. NIST SP 800-31, Intrusion Detection Systems.

b. NIST SP 800-41, Guides on Firewalls and Firewall Policy.

c. NIST SP 800-44, Guidelines on Securing Public Web Servers.

d. NIST SP 800-45, Guidelines on Electronic Mail Security.

e. NIST SP 800-46, Telecommuting and Broadband Communications.

f. NIST SP 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices.

g. NIST SP 800-58, Security Considerations for Voice Over IP Systems.

h. NIST SP 800-77, Guide to IP Sec VPNs.

11.3.13.5 All NASA networks, including wireless networks, shall:

a. Be either part of a subordinate SSP or be a subordinate system under the OAIT master system for networking.

b. Describe their security controls in their SSP and identify in the Risk Assessment Summary any residual risks that are to be accepted by the AO.

c. Be managed in accordance with NASA's SOPs on network and wireless network security.

11.3.13.6 Networks operated and managed under contracts, cooperative agreements, grants, partnership agreements, agreements with international partners, university partners and other educational entities, NASA Space Act Agreements, and special volunteer partners shall establish configuration control of their networks, document modifications to the approved configurations, and notify their customers of changes to the security controls.

11.3.13.7 All network operations shall document all approved network devices making up the network and connected systems and monitor for unapproved devices and systems.

11.3.13.8 Remote connection to NASA networks from an Internet Service Provider (ISP) shall require encrypted authentication and data transmission, such as by a Virtual Private Network (VPN).

11.3.13.9 Remote privileged access to a NASA system from outside NASA network space shall require two-factor authentication and encrypted data transmission.

11.3.13.10 Each Center shall have a NCCB that shall:

a. Conduct a risk assessment for modifications to the network.

b. Approve or disapprove all proposed modifications.

c. Provide notification to its customers of all modifications that would affect the protections provided by the network.

d. Document all Center NCCB actions and, if appropriate, ensure that the affected SSPs are updated and the AO notified for possible recertification and reaccreditation prior to the modification being implemented.

e. Have the authority to disconnect or deny service to any network-attached device, including wireless devices, in the event of an incident or violation of the rules of the systems or acceptable use policy.

11.3.14 Penetration Testing

11.3.14.1 A security penetration test is an activity in which a test team attempts to circumvent the security processes and controls of a computer system to include social engineering. Posing as either internal or external unauthorized intruders, the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the target computer in unauthorized ways. Due to the sensitive nature of the testing, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results.

11.3.14.2 Penetration Testing Requirements

11.3.14.3 NASA shall ensure that penetration testing is conducted only in conjunction with the Center CIO, the Center ITSM, the affected system administrator's network operation, and IT security staff and will be performed in a spirit of a joint training exercise by all participants.

11.3.14.4 Penetration testing shall follow ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting.

11.3.14.5 The OCIO or cognizant Center CIO shall approve all penetration testing run against NASA IP address space.

11.3.14.6 Results from penetration testing shall be considered ACI or SBU information and will be handled and protected accordingly.

11.3.14.7 Rules of engagement must be agreed to, documented, and signed by all parties prior to the initiation of penetration testing following ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting.

11.3.14.8 A non-disclosure agreement shall be signed by a non-NASA reviewer.

11.3.15 System and Communication Protection Requirements

11.3.15.1 For unclassified IT resources, NASA shall comply with National policy by ensuring that all valuable information and information systems are afforded an adequate degree of protection that is commensurate with the risks posed to NASA IT resources and the magnitude of potential harm that could be experienced by NASA if IT resources are compromised or sensitive information is inadvertently disclosed. To achieve this goal, NASA has established standards for encryption and digital signatures in NASA STD 2820, Encryption and Digital Signature Standards. NASA management shall comply with NIST FIPS Publication 140-2, Security Requirements for Cryptographic Modules, FIPS Publication 46-3, Data Encryption Standard and NIST SP 800-77, Guide to IPSec VPNs. Specific NASA requirements follow.

11.3.15.2 Only National Security Agency (NSA) approved and endorsed encryption products and/or techniques shall be used for protecting all telemetry and telecommunications involving:

a. Radio transmissions or signals for command/destruct uplinks to launch vehicles, spacecraft, test aircraft, and other manned or unmanned aerospace vehicles.

b. Commanding of command and control links to vehicles for vehicle housekeeping activities.

c. Payload operations including command and control of the payload and the handling of raw data from spacecraft payloads.

11.3.15.3 The encryption level, strength, and type shall be based upon risk and cost assessments conducted by the program or project management and will be NSA and/or NIST-approved and endorsed encryption products and/or techniques.

11.3.15.4 All NASA PCAs shall address the requirement for data encryption and document the decision and the determination of the type, level, and strength of the encryption that will be used.

11.3.15.5 All command/destruct uplinks to launch vehicles, spacecraft, test aircraft, and other manned or unmanned aerospace vehicles shall utilize NSA and/or NIST-approved or endorsed techniques and products. Waivers/variances/exceptions to the requirement to use NSA and/or NIST products shall be considered on a case-by-case basis and submitted to the OSPP with concurrence by the OCIO.

11.3.15.6 All command and control links to vehicles for vehicle housekeeping activities shall:

a. Utilize NSA and/or NIST-approved or endorsed techniques and products.

b. Waivers/variances/exceptions to the requirement to use NSA and/or NIST products shall be considered on a case-by-case basis and shall be submitted to the OSPP for approval with concurrence by the OCIO.

11.3.15.7 All payload operations including command and control of the payload and the handling of raw data from spacecraft payloads shall:

a. Utilize NSA and/or NIST-approved or endorsed techniques and products.

b. Waivers/variances/exceptions to the requirement to use NSA and/or NIST products shall be considered on a case-by-case basis and shall be submitted to the OSPP for approval with concurrence by the OCIO.

11.3.15.8 NASA systems and applications whose information security category is rated high or moderate (see Chapter 7, System Characterization, Information Categorization, System Types, and System Boundaries) shall:

a. Be evaluated for the impact of not utilizing encryption as a security control by considering not only the value of information and the cost of recovery, but also the intangible costs of possible harm or loss, which may equal or outweigh, the measurable costs.

b. Document the decision to use or not to use encryption in the SSP.

c. If the decision is to use encryption, utilize NSA and/or NIST-approved or endorsed techniques and products.

11.3.15.9 ACI or SBU information, as determined by NPR 1600.1, NASA Security Program Procedural Requirements, shall be encrypted in transmission and shall:

a. Utilize NSA and/or NIST-approved or endorsed techniques and products.

b. Waivers/variances/exceptions to the requirement to use NSA and/or NIST products shall be considered on a case-by-case basis and shall be submitted to the OSPP for approval with concurrence by the OCIO.

11.4 Additional Security Controls References

a. NPR 1441.1, Records Retention Schedule.

b. NPD 1382.17, Privacy Act - Internal NASA Direction in Furtherance of NASA Regulations.

c. NPD 1600.2 NASA Security Program Policy.

d. NPR 1600.6 Communications Security Procedures and Guidelines.

e. NPR 1620.1, Security Procedures and Guidelines.

f. NPD 2110.1, Foreign Access to NASA Technology Transfer Materials.

g. NPD 2190.1, NASA Export Control Program.

h. NPR 2200.2, Guidelines for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information.

i. NPR 2210.1, External Release of NASA Software.

j. NPD 2220.5, Management of NASA Scientific and Technical Information (STI).

k. NPR 2800.1, Managing Information Technology.

l. NPD 2810.1, NASA Information Security.

m. NPD 2820.1, NASA Software Policy.

n. NPD 7120.4, Program/Project Management.

o. NPR 7120.5, NASA Program and Project Management Processes and Requirements.

p. NPR 7150.2, Software Engineering Requirements.

q. NASA Technical Standards, Series 2800, Computer Systems, Software, Information Systems.

r. NASA's E-FOIA Regulations, 64 Federal Register 39,401-39,414 (1999) (codified at 14 CFR Part 1206).

s. NIST SP 800-12, Introduction to Computer Security: The NIST Handbook: Computer Support and Operations Requirements.

t. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.

u. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems.

v. NIST SP 800-27, Engineering Principles for IT Security.

w. NIST SP 800-28, Guidelines on Active Content and Mobile Code.

x. NIST SP 800-31, Intrusion Detection Systems.

y. NIST SP 800-41, Guides on Firewalls and Firewall Policy.

x. NIST SP 800-42, Guidelines on Network Security Testing.

aa. NIST SP 800-44, Guidelines on Securing Public Web Servers.

ab. NIST SP 800-45, Guidelines on Electronic Mail Security.

ac. NIST SP 800-46, Telecommuting and Broadband Communications.

ad. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.

ae. NIST SP 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices.

af. NIST SP 800-77, Guide to IP Sec VPNs.

ag. Attorney General Policy Memorandum of October 12, 2001 on the Freedom of Information Act, Appropriate Account and Use of IT Resources.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS